Manual Penetration Testing

1. Manual Penetration Testing
2. Veracode DevOps Penetration Testing
3. Veracode Time-Boxed Manual Penetration Testing
4. Requesting Veracode Manual Penetration Testing

1 | Manual Penetration Testing

You can conduct a manual penetration assessment to observe the application in a runtime environment and simulate real-world attack scenarios. Penetration testing includes efforts to:

- Identify design flaws.
- Exploit vulnerabilities.
- Leverage combinations of lower impact flaws into higher impact vulnerabilities.
- Determine if identified flaws affect the confidentiality, integrity, or availability of the application.

The objectives of a web-focused penetration assessment include testing using proprietary or public tools to:

- Assess how vulnerabilities might be exploited against a target while establishing a running profile of attack methods discovered.
- Execute test cases to confirm the vulnerability and attempt to determine the impact to business.
- Customize and expand attack payloads, accounting for the specifics of the implementation of the target and environment.
- Analyze captured data for vulnerability patterns, interpreting the results, and developing remediation recommendations.

Human testers identify unorthodox ways of attacking applications and infrastructures to understand the design and functionality, complex authorization processes, and business logic requirements that might not be possible for computing systems to replicate today. These insights enable developers to secure their applications and infrastructure against a broader range of attacks.

Veracode recommends that your organization utilize Veracode Manual Penetration Testing in conjunction with other automated security assessments such as Veracode Static Analysis, Dynamic Analysis, and SCA to ensure maximum coverage from your security program.

Veracode uses industry standards for classifying and reporting manual penetration test vulnerabilities, including:

- Common Vulnerability Scoring System (CVSS) v3
- Common Weakness Enumeration (CWE)
- Common Attack Pattern Enumeration and Classification (CAPEC)

Details of Veracode Manual Penetration Testing are available in the methodology section of the Veracode Detailed PDF Report and Customizable PDF Report.

Veracode performs all Manual Penetration Testing according to industry-standard testing methodologies where applicable. The following table describes testing types, methodologies, and

vulnerability types that form the foundation of Veracode manual penetration testing.

Test Type	Methodology	Vulnerabilities
Web application/API	PTES (Penetration Testing Execution Standard), OWASP Testing Guide	OWASP Top 10 and CWE Top 25
Mobile application	PTES (Penetration Testing Execution Standard), OWASP Mobile Security Testing Guide	OWASP Mobile Top 10
Desktop or thick-client applications	PTES (Penetration Testing Execution Standard), OWASP recommended testing guidance and best practices	• Application Logic • Code Injection • Local Storage • Binary Exploitation and Reverse Engineering • Excessive Privileges • Unencrypted Storage of Sensitive Information • Unencrypted Transmission of Sensitive Information • Weak Encryption Implementations • Weak Assembly Controls • Weak GUI Controls • Weak or Default Passwords
Internet of things (IoT) and embedded systems	PTES (Penetration Testing Execution Standard), OWASP IoT Testing Guide and other industry best practices	OWASP IoT Top 10

Test Type	Methodology	Vulnerabilities
Infrastructure and Operations (DevOps Penetration Testing)	PTES (Penetration Testing Execution Standard), NIST SP 800-115, PCI DSS 11.3 (for PCI engagements)	Can vary depending on scope and rules of engagement

2 | Veracode DevOps Penetration Testing

In addition to performing manual testing for an application, Veracode DevOps Penetration Testing can evaluate the following areas:

Infrastructure

- Datacenter attack surfaces (proprietary or cloud-based) including:
  - Architecture that hosts applications
  - Border-security devices
  - Communication systems (PBX, routing)
  - Unknown or 'rogue' servers or services
- Microservices and related interactions
- Searches for major sources of data leaks and breaches, such as:
  - Misconfigured AWS S3 buckets
  - Exposed MongoDB instances
  - Elasticsearch databases

  Veracode DevOps Penetration Testing also uses Open Source Intelligence (OSINT) techniques to locate vulnerabilities in the infrastructure.

Application Developers

- Use of Open Source Intelligence (OSINT) techniques to conduct GitHub repository and Stackoverflow analysis for:
  - Exposed credentials
  - Exposed sensitive data related to application development
  - Job boards
  - Other potential problem areas
- Locating information that could be used for targeted phishing or social engineering attacks on developers and the organization

Veracode DevOps Penetration Testing meets PCI DSS 11.3 and GDPR Article 32 compliance requirements.

3 | Veracode Time-Boxed Manual Penetration Testing

In some situations, timing restraints, budgetary considerations, or strategic planning purposes may require limiting the level of effort for penetration testing.

In cases where time is constrained, Veracode focuses on providing the most value for the time allotted. Veracode Penetration Testers may choose to customize the methodology to focus on high-priority, business-relevant flaws. For example, the tester may choose to focus on finding representative examples of higher risk flaws such as injection, authentication, and authorization flaws.

4 | Requesting Veracode Manual Penetration Testing

To request Veracode Manual Penetration Testing, contact your Veracode account manager or Sales team.

After the testing is complete, results are available in a dedicated MPT portal which you can download in PDF, Word, or CSV format.